Таким образом, рассмотрены правовые аспекты, регламентирующие процесс исследования накопителей информации. Приведены примеры деструктивных воздействий на устройства хранения информации. Представлены базовые механизмы предотвращения подобного рода воздействий.

Список литературы

1. *Bell G.*, *Boddington R.* Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery? Murdoch University, 2010.

2. *Федотов Н. Н.* Форензика — компьютерная криминалистика. М. : Юр. мир, 2007.

3. Федеральный закон от 28 июля 2012 г. № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».

4. Уголовно-процессуальный кодекс Российской Федерации (ред. от 29.07.2017).

5. Стандарт Банка России СТО БР ИББС-1.3–2016. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств. Москва, 2016.

6. ACPO Good Practice Guide for Digital Evidence v5 (latest). ACPO, 2012.

7. Hardware Write Block [Электронный ресурс]. Режим доуступа: https://www.cftt.nist.gov/hardware_write_block.htm (дата обращения: 06.11.2017)

8. Write Blockers Block [Электронный ресурс], режим доуступа: http://www.forensicswiki.org/wiki/Write_Blockers (дата обращения: 06.11.2017).

УДК 004.056.53

И. Ф. Файсханов
Научный руководитель: д-р тех. наук, проф. Л. Г. Доросинский
Уральский федеральный университет, Екатеринбург

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ УСТОЙЧИВОГО КЛАВИАТУРНОГО ПОЧЕРКА

Аннотация. В данной работе основное внимание уделяется процессу аутентификации пользователей с помощью устойчивого клавиатурного почерка.

Данная тематика является перспективной и актуальной, поскольку вопросы безопасности информации всегда имеют высокий приоритет, особенно, если защищаемая информация представляет какую-либо ценность.

Проанализирован алгоритм работы системы аутентификации, приведенный в более ранней публикации. Приведены результаты текущих исследований клавиатурного почерка, а также о дальнейших планах по модернизации данной системы.

Ключевые слова: информационная безопасность; аутентификация; идентификация; биометрические данные; временные характеристики.

Введение

Как известно, правоохранительные органы долгое время работают успешно с одним из типов поведенческих биометрических данных — рукописным почерком. Высота, длина, углы букв — это не полный перечень характеристик, по которым можно идентифицировать человека, который написал тот или иной текст.

Однако прогресс не стоит на месте, и глобальная информатизация ознаменовала переход к новому обществу — информационному. То, что делалось вручную или механически, начало осуществляться автоматически при участии оператора. Но тем не менее работа человека и машины аналогично характеризуется поведенческими биометрическими данными.

Одними из таких характеристик являются биометрические характеристики ввода с клавиатуры текста, иначе говоря, клавиатурный почерк.

Система аутентификации по клавиатурному почерку

Принцип работы системы аутентификации пользователей подробно рассмотрен в [1]. Стоит привести метод работы системы (рис. 1).

В перспективе рассматривается разработка системы, действующей по данному алгоритму, а также внедрение анализа характеристик манипулятора «мышь».

В ходе первых экспериментов с данной системой участие приняли пять испытуемых. Задача каждого оператора была ввести пять раз фразу «В чащах юга жил бы цитрус? Да, но фальшивый экземпляр!»

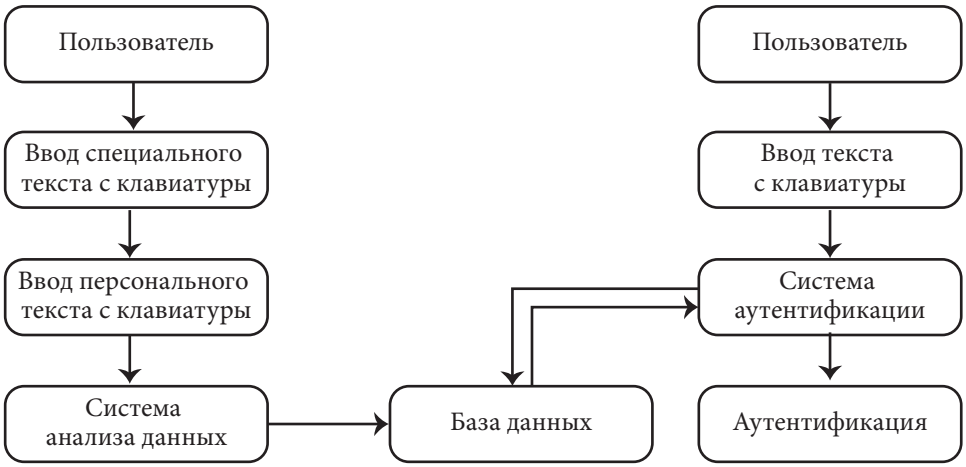

Рис. 1. Принцип работы системы аутентификации

Дальнейшая задача — анализ корреляции определенной длительности: сколько раз встречается та или иная длительность ввода с учетом погрешности 30 мс.

Данные значения приняты за индивидуальную характеристику оператора.

Ниже приведены индивидуальные характеристики операторов № 1–№ 5 на одном графике (рис. 2).

По оси абсцисс — длительность в мс, по оси ординат — количество повторений определенной усредненной длительности ввода.

Стоит отметить, что на 200 мс обнаружено большое количество совпадений. Это можно объяснить опытностью операторов. Для дальнейшего развития системы стоит отметить данный факт и рассматривать временные характеристики с более точным фильтром.

Полученные данные сохраняются в базу данных, дальнейшей задачей которой является аутентифицировать оператора, исходя из имеющегося массива данных.

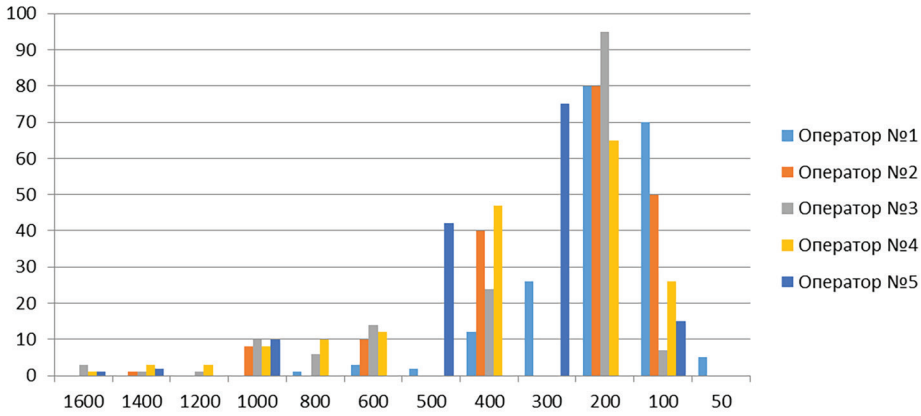

Рис. 2. Индивидуальные характеристики операторов № 1–№ 5

Заключение

Таким образом, подводя итоги, можно отметить, что простейшим, а также надежным, при соблюдении определенных требований, и наиболее популярным средством аутентификации в данный момент является пароль. Однако прогресс не стоит на месте, и, возможно, пароль как таковой уступит место иным средствам аутентификации, которые не будут иметь таких существенных недостатков, как его потеря или хранение в доступном месте, записанном на что-либо. И сам процесс аутентификации будет происходить незаметно для пользователя.

По данной работе на текущий момент имеются следующие результаты:

1) сделаны выводы относительно актуальности и важности исследований;

2) разработан и внедрен алгоритм идентификации оператора;
3) получены первые экспериментальные результаты.

Список литературы

1. *Файсханов И. Ф.* Основы управления процессом аутентификации пользователей в социальных и экономических системах : сб. докладов X Международ. конф. «Российские регионы в фокусе перемен». Екатеринбург, 2015. С. 1108–1112.

УДК 004.056

И. А. Шевяков
Научный руководитель: канд. тех. наук, доц. А. Н. Соколов
Южно-Уральский государственный университет, Челябинск

АНАЛИЗ АКТУАЛЬНЫХ УЯЗВИМОСТЕЙ SCADA-СИСТЕМ

Аннотация. В работе рассматриваются актуальные типы уязвимостей программного обеспечения диспетчерского контроля и сбора данных АСУ ТП. Приводится обзор состояния выявления и устранения угроз безопасности АСУ ТП и SCADA-систем в мире, а также основные их типы.

Ключевые слова: защита информации; безопасность АСУ ТП; уязвимость SCADA.

В течение последних десятилетий атаки на АСУТП становятся привлекательной целью, наблюдается значительный рост целенаправленных атак на промышленные информационные системы с целью промышленного шпионажа, мошенничества и нарушения функционирования предприятия. Так, например, на смену отдельным «червям» Stuxnet (2010) и Flame (2012) пришли более изощренные схемы многоступенчатых атак. А для распространения трояна Havex в 2014 г. хакеры взламывали сайты производителей программного обеспечения для управления промышленными предприятиями (SCADA) и заражали официальные дистрибутивы SCADA-систем, которые затем устанавливались на предприятиях, что позволило злоумышленникам получить контроль над системами управления в нескольких европейских странах.

Обзор состояния безопасности АСУ ТП, проведенный компанией Positive Technologies в 2012 г., показал довольно тревожную картину [1, 2]. Резко увеличивается число обнаруженных уязвимостей. С 2010 по 2012 г. установлено в 20 раз больше уязвимостей, чем за предыдущие 5 лет. Каждая пятая уязви-